Configurer l'ASA pour transmettre le trafic IPv6

Contenu

Introduction

Ce document décrit comment configurer le dispositif de sécurité adaptatif Cisco (ASA) afin de transmettre le trafic IPv6 (Internet Protocol Version 6) dans ASA Versions 7.0(1) et ultérieures.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur les versions 7.0(1) et ultérieures de Cisco ASA.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Actuellement, l'IPv6 est encore relativement nouveau en termes de pénétration du marché. Cependant, les demandes d'assistance et de dépannage relatives à la configuration IPv6 ont augmenté de façon constante. Le présent document a pour objet de répondre à ces besoins et de fournir :

- Présentation générale de l'utilisation d'IPv6
- Configurations IPv6 de base sur l'ASA
- Informations sur le dépannage de la connectivité IPv6 via l'ASA
- Une liste des problèmes et solutions IPv6 les plus courants, tels qu'identifiés par le centre d'assistance technique Cisco (TAC)

Note: Étant donné que le protocole IPv6 n'en est qu'à ses débuts en tant que remplacement IPv4 à l'échelle mondiale, ce document sera périodiquement mis à jour afin de conserver précision et pertinence.

Informations sur les fonctionnalités IPv6

Voici quelques informations importantes sur la fonctionnalité IPv6 :

- Le protocole IPv6 a été introduit pour la première fois dans ASA version 7.0(1).
- La prise en charge d'IPv6 en mode transparent a été introduite dans ASA version 8.2(1).

Présentation d'IPv6

Le protocole IPv6 a été développé entre le milieu et la fin des années 1990, principalement en raison du fait que l'espace d'adressage IPv4 public s'est rapidement réduit. Bien que la traduction d'adresses de réseau (NAT) ait considérablement aidé IPv4 et retardé ce problème, il est devenu indéniable qu'un protocole de remplacement serait éventuellement nécessaire. Le protocole IPv6 a été officiellement détaillé dans la RFC 2460 en décembre 1998. Vous pouvez en savoir plus sur le protocole dans le document officiel RFC 2460, situé sur le site Internet de l'IETF (Internet Engineering Task Force).

Améliorations IPv6 sur IPv4

Cette section décrit les améliorations apportées au protocole IPv6 par rapport à l'ancien protocole IPv4.

Capacités d'adressage étendues

Le protocole IPv6 fait passer la taille de l'adresse IP de 32 bits à 128 bits afin de prendre en charge plus de niveaux de hiérarchie d'adressage, un nombre beaucoup plus grand de noeuds adressables et une configuration automatique des adresses plus simple. L'évolutivité du routage de multidiffusion est améliorée par l'ajout d'un champ d'*étendue* aux adresses de multidiffusion. En outre, un nouveau type d'adresse, appelé *adresse anycast*, est défini. Ceci est utilisé afin d'envoyer un paquet à n'importe quel noeud d'un groupe.

Simplification du format d'en-tête

Certains champs d'en-tête IPv4 ont été supprimés ou rendus facultatifs afin de réduire le coût de traitement des paquets dans les cas courants et de limiter le coût de bande passante de l'en-tête IPv6.

Prise en charge améliorée des extensions et des options

Les modifications apportées au codage des options d'en-tête IP permettent un transfert plus

efficace, des limites moins strictes sur la longueur des options et une plus grande flexibilité pour l'introduction de nouvelles options à l'avenir.

Fonctionnalité d'étiquetage de flux

Une nouvelle fonctionnalité est ajoutée afin d'activer l'étiquetage des paquets qui appartiennent à des *flux de* trafic spécifiques pour lesquels l'expéditeur demande une gestion spéciale, comme la qualité de service (QoS) non par défaut ou le service *en temps réel*.

Fonctionnalités d'authentification et de confidentialité

Les extensions utilisées pour prendre en charge l'authentification, l'intégrité des données et la confidentialité des données (facultative) sont spécifiées pour IPv6.

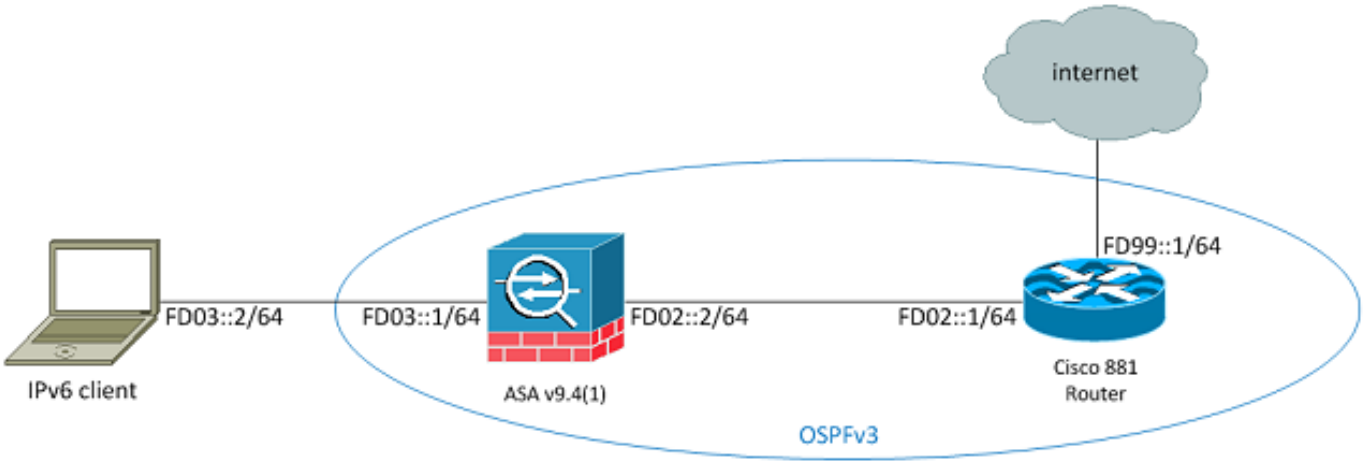
Configuration

Cette section décrit comment configurer Cisco ASA pour l'utilisation d'IPv6.

> **Note**: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Il s'agit de la topologie IPv6 pour les exemples utilisés dans ce document :



Configuration des interfaces pour IPv6

Pour transmettre le trafic IPv6 via un ASA, vous devez d'abord activer IPv6 sur au moins deux interfaces. Cet exemple décrit comment activer IPv6 afin de transmettre le trafic de l'interface interne sur **Gi0/0** à l'interface externe sur **Gi0/1** :

```
ASAv(config)# interface GigabitEthernet0/0
ASAv(config-if)# ipv6 enable

ASAv(config)# interface GigabitEthernet0/1
ASAv(config-if)# ipv6 enable
```

Vous pouvez maintenant configurer les adresses IPv6 sur les deux interfaces.

> **Note**: Dans cet exemple, les adresses de l'espace ULA (Unique Local Addresses) de fc00::/7 sont utilisées, de sorte que toutes les adresses commencent par **FD** (comme, fdxx:xxxx:xxxx....). En outre, lorsque vous écrivez des adresses IPv6, vous pouvez utiliser des deux-points (**::**) afin de représenter une ligne de zéros pour que **FD01::1/64** soit identique à **FD01:0000:000:0000:000:0 000:000:00001**.

```
ASAv(config)# interface GigabitEthernet0/0
ASAv(config-if)# ipv6 address fd03::1/64
ASAv(config-if)# nameif inside
ASAv(config-if)# security-level 100

ASAv(config)# interface GigabitEthernet0/1
ASAv(config-if)# ipv6 address fd02::2/64
ASAv(config-if)# nameif outside
ASAv(config-if)# security-level 0
```

Vous devez maintenant disposer de la connectivité de base de couche 2 (L2)/couche 3 (L3) à un routeur en amont sur le VLAN externe à l'adresse **fd02::1** :

```
ASAv(config-if)# ping fd02::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to fd02::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Configuration du routage IPv6

Tout comme avec IPv4, même s'il existe une connectivité IPv6 avec les hôtes sur le sous-réseau directement connecté, vous devez toujours disposer des routes vers les réseaux externes pour savoir comment les atteindre. Le premier exemple montre comment configurer une route statique par défaut afin d'atteindre tous les réseaux IPv6 via l'interface externe avec une adresse de tronçon suivant **fd02::1**.

Configuration du routage statique pour IPv6

Utilisez ces informations afin de configurer le routage statique pour IPv6 :

```
ASAv(config)# ipv6 route outside 0::0/0 fd02::1
ASAv(config)# show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, B - BGP
```

```
L fd02::2/128 [0/0]
via ::, outside
C fd02::/64 [0/0]
via ::, outside
L fd03::1/128 [0/0]
via ::, inside
C fd03::/64 [0/0]
via ::, inside
L fe80::/10 [0/0]
via ::, inside
via ::, outside
L ff00::/8 [0/0]
via ::, inside
via ::, outside
S   ::/0 [1/0]
via fd02::1, outsideASAv(config)#
```

Comme l'illustre l'illustration, il existe maintenant une connectivité à un hôte sur un sous-réseau externe :

```
ASAv(config)# ping fd99::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to fd99::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ASAv(config)#
```

> **Note**: Si vous souhaitez utiliser un protocole de routage dynamique pour gérer le routage IPv6, vous pouvez également le configurer. Ceci est décrit dans la section suivante.

Configuration du routage dynamique pour IPv6 avec OSPFv3

Tout d'abord, vous devez examiner la configuration OSPFv3 (Open Shortest Path First Version 3) sur le routeur à services intégrés (ISR) de la gamme Cisco 881 en amont :

```
C881#show run | sec ipv6
ipv6 unicast-routing

!--- This enables IPv6 routing in the Cisco IOS®.

.....
ipv6 ospf 1 area 0
address-family ipv6 unicast
passive-interface default
no passive-interface Vlan302

!--- This is the interface to send OSPF Hellos to the ASA.

default-information originate always

!--- Always distribute the default route.

redistribute static
ipv6 route ::/0 FD99::2

!--- Creates a static default route for IPv6 to the internet.
```

Voici la configuration d'interface appropriée :

```
C881#show run int Vlan302
interface Vlan302
....
ipv6 address FD02::1/64
ipv6 ospf 1 area 0
C881#
```

Vous pouvez utiliser des captures de paquets ASA afin de vérifier que les paquets *Hello* OSPF sont vus depuis le routeur de service intégré sur l'interface externe :

```
ASAv(config)# show run access-list test_ipv6
access-list test_ipv6 extended permit ip any6 any6
ASAv(config)# show cap
capture capout type raw-data access-list test_ipv6 interface outside
[Capturing - 37976 bytes]
ASAv(config)# show cap capout

367 packets captured

1: 11:12:04.949474 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
neighbor sol: who has fe80::250:56ff:fe9d:34a8 [class 0xe0]
2: 11:12:06.949444 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
neighbor sol: who has fe80::250:56ff:fe9d:34a8 [class 0xe0]
   3: 11:12:07.854768       fe80::c671:feff:fe93:b516 > ff02::5: ip-proto-89 40
[hlim 1]
4: 11:12:07.946545 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
neighbor sol: who has fe80::250:56ff:fe9d:34a8 [class 0xe0]
5: 11:12:08.949459 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
neighbor sol: who has fe80::250:56ff:fe9d:34a8 [class 0xe0]
6: 11:12:09.542772 fe80::217:fff:fe17:af80 > ff02::5: ip-proto-89 40
[hlim 1]
....
  13: 11:12:16.983011       fe80::c671:feff:fe93:b516 > ff02::5: ip-proto-89 40
[hlim 1]
14: 11:12:18.947170 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
neighbor sol: who has fe80::250:56ff:fe9d:34a8 [class 0xe0]
15: 11:12:19.394831 fe80::217:fff:fe17:af80 > ff02::5: ip-proto-89 40
[hlim 1]
16: 11:12:19.949444 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
  21: 11:12:26.107477       fe80::c671:feff:fe93:b516 > ff02::5: ip-proto-89 40
[hlim 1]
ASAv(config)#
```

Dans la capture de paquets précédente, vous pouvez voir que les paquets OSPF (ip-proto-89) arrivent de l'adresse link-local IPv6, qui correspond à l'interface correcte sur le routeur de service intégré :

```
C881#show ipv6 interface brief
......
Vlan302 [up/up]
    FE80::C671:FEFF:FE93:B516
FD02::1
C881#
```

Vous pouvez maintenant créer un processus OSPFv3 sur l'ASA afin d'établir une contiguïté avec l'ISR :

```
ASAv(config)# ipv6 router ospf 1
ASAv(config-rtr)# passive-interface default
```

```
ASAv(config-rtr)# no passive-interface outside
ASAv(config-rtr)# log-adjacency-changes
ASAv(config-rtr)# redistribute connected
ASAv(config-rtr)# exit
```

Appliquez la configuration OSPF à l'interface externe ASA :

```
ASAv(config)# interface GigabitEthernet0/1
ASAv(config-if)# ipv6 ospf 1 area 0
ASAv(config-if)# end
```

Cela devrait amener l'ASA à envoyer les paquets Hello OSPF de diffusion sur le sous-réseau IPv6. Entrez la commande **show ipv6 ospf neighbor** afin de vérifier la contiguïté avec le routeur :

```
ASAv# show ipv6 ospf neighbor

Neighbor ID Pri State Dead Time Interface ID Interface
    14.38.104.1 1     FULL/BDR        0:00:33     14              outside
```

Vous pouvez également confirmer l'ID de voisin sur le routeur de service intégré, car il utilise par défaut l'adresse IPv4 configurée la plus élevée pour l'ID :

```
C881#show ipv6 ospf 1
 Routing Process "ospfv3 1" with ID 14.38.104.1
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an autonomous system boundary router
Redistributing External Routes from,
static
 Originate Default Route with always

!--- Notice the other OSPF settings that were configured.

Router is not originating router-LSAs with maximum metric
....

C881#
```

L'ASA doit maintenant avoir appris la route IPv6 par défaut à partir du routeur de service intégré. Afin de confirmer cela, entrez la commande **show ipv6 route** :

```
ASAv# show ipv6 route

IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, B - BGP
O 2001:aaaa:aaaa:aaaa::/64 [110/10]
via ::, outside
L fd02::2/128 [0/0]
via ::, outside
C fd02::/64 [0/0]
via ::, outside
L fd03::1/128 [0/0]
via ::, inside
C fd03::/64 [0/0]
via ::, inside
L fe80::/10 [0/0]
via ::, inside
via ::, outside
```

```
L ff00::/8 [0/0]
via ::, inside
via ::, outside
OE2  ::/0 [110/1], tag 1

!--- Here is the learned default route.

    via fe80::c671:feff:fe93:b516, outside
ASAv#
```

La configuration de base des paramètres d'interface et des fonctions de routage pour IPv6 sur l'ASA est maintenant terminée.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Les procédures de dépannage de la connectivité IPv6 suivent la plupart des méthodes utilisées pour dépanner la connectivité IPv4, avec quelques différences. Du point de vue du dépannage, l'une des différences les plus importantes entre IPv4 et IPv6 est que le protocole ARP (Address Resolution Protocol) n'existe plus dans IPv6. Au lieu d'utiliser ARP pour résoudre les adresses IP sur le segment LAN local, IPv6 utilise un protocole appelé ND (Neighbor Discovery).

Il est également important de comprendre que ND exploite le protocole ICMPv6 (Internet Control Message Protocol Version 6) pour la résolution d'adresse MAC (Media Access Control). Pour plus d'informations sur IPv6 ND, reportez-vous au guide de configuration IPv6 ASA dans la section Découverte de voisin IPv6 du *livret 1 CLI : Guide de configuration de l'interface de ligne de commande des opérations générales de la gamme Cisco ASA, version 9.4* ou dans RFC 4861.

Àl'heure actuelle, la plupart des problèmes de dépannage liés à IPv6 impliquent des problèmes de configuration de réseau, de routage ou de sous-réseau. Cela est probablement dû au fait que ce sont également les principales différences entre IPv4 et IPv6. Le ND fonctionne différemment du protocole ARP, et l'adressage réseau interne est également très différent, car l'utilisation de la NAT est fortement déconseillée dans IPv6 et l'adressage privé n'est plus exploité comme il l'était dans IPv4 (après RFC 1918). Une fois que ces différences sont comprises et/ou que les problèmes de couche 2/couche 3 sont résolus, le processus de dépannage au niveau de la couche 4 (couche 4) et au-dessus est essentiellement identique à celui utilisé pour IPv4, car les protocoles TCP/UDP et de couche supérieure fonctionnent essentiellement de la même manière (quelle que soit la version IP utilisée).

Dépannage de la connectivité de couche 2 (ND)

La commande la plus basique utilisée pour dépanner la connectivité de couche 2 avec IPv6 est la commande **show ipv6 neighbor [nameif]**, qui est l'équivalent de la commande **show arp** pour IPv4.

Voici un exemple de résultat :

```
ASAv(config)# show ipv6 neighbor outside
IPv6 Address Age Link-layer Addr State Interface
fd02::1                                   0 c471.fe93.b516  REACH   outside
fe80::c671:feff:fe93:b516                32 c471.fe93.b516  DELAY   outside
fe80::e25f:b9ff:fe3f:1bbf 101 e05f.b93f.1bbf STALE outside
fe80::b2aa:77ff:fe7c:8412 101 b0aa.777c.8412 STALE outside
fe80::213:c4ff:fe80:5f53 101 0013.c480.5f53 STALE outside
fe80::a64c:11ff:fe2a:60f4 101 a44c.112a.60f4 STALE outside
fe80::217:fff:fe17:af80 99 0017.0f17.af80 STALE outside
ASAv(config)#
```

Dans cette sortie, vous pouvez voir la résolution réussie de l'adresse IPv6 de **fd02::1**, qui appartient au périphérique avec l'adresse MAC **c471.fe93.b516**.

> **Note**: Vous remarquerez peut-être que la même adresse MAC d'interface de routeur apparaît deux fois dans la sortie précédente, car le routeur a également une adresse link-local auto-attribuée pour cette interface. L'adresse link-local est une adresse spécifique au périphérique qui ne peut être utilisée que pour la communication sur le réseau directement connecté. Les routeurs ne transfèrent pas les paquets via des adresses link-local, mais ils ne servent qu'à la communication sur le segment de réseau directement connecté. De nombreux protocoles de routage IPv6 (tels que OSPFv3) utilisent des adresses link-local afin de partager des informations de protocole de routage sur le segment L2.

Afin d'effacer le cache ND, entrez la commande **clear ipv6 neighbors**. Si le ND échoue pour un hôte particulier, vous pouvez entrer la commande **debug ipv6 nd**, ainsi que procéder à des captures de paquets et vérifier les syslogs, afin de déterminer ce qui se produit au niveau de L2. N'oubliez pas que le ND IPv6 utilise des messages ICMPv6 afin de résoudre les adresses MAC pour les adresses IPv6.

IPv4 ARP contre IPv6 ND

Considérez cette table de comparaison des protocoles ARP pour IPv4 et ND pour IPv6 :

ARP IPv4	ND IPv6
REQUÊTE ARP (Qui a 10.10.10.1 ?)	Sollicitation de voisin
RÉPONSE ARP (10.10.10.1 est à dead.dead.dead.dead)	Annonce de voisin

Dans le scénario suivant, le ND ne parvient pas à résoudre l'adresse MAC de l'hôte *fd02::1* situé sur l'interface externe.

Débogues ND

Voici la sortie de la commande **debug ipv6 nd** :

```
ICMPv6-ND: Sending NS for fd02::1 on outside

!--- "Who has fd02::1"

ICMPv6-ND: Sending NS for fd02::1 on outside
ICMPv6-ND: Sending NS for fd02::1 on outside
ICMPv6-ND: INCMP deleted: fd02::1
ICMPv6-ND: INCMP -> DELETE: fd02::1
```

```
ICMPv6-ND: DELETE -> INCMP: fd02::1
ICMPv6-ND: Sending NS for fd02::1 on outside
ICMPv6-ND: Sending NS for fd02::1 on outside
ICMPv6-ND: Sending NA for fd02::2 on outside

!--- "fd02::2 is at dead.dead.dead"

ICMPv6-ND: Sending NS for fd02::1 on outside
ICMPv6-ND: INCMP deleted: fd02::1
ICMPv6-ND: INCMP -> DELETE: fd02::1
ICMPv6-ND: DELETE -> INCMP: fd02::1

!--- Here is where the ND times out.

ICMPv6-ND: Sending NS for fd02::1 on outside
ICMPv6-ND: Sending NS for fd02::1 on outside
```

Dans cette sortie de débogage, il *apparaît* que les annonces de voisinage de **fd02::2** ne sont jamais reçues. Vous pouvez vérifier les captures de paquets afin de confirmer si c'est vraiment le cas.

Captures de paquets ND

> **Note**: Depuis la version 9.4(1) d'ASA, les listes d'accès sont toujours requises pour les captures de paquets IPv6. Une demande d'amélioration a été déposée afin de suivre ceci avec l'ID de bogue Cisco CSCtn09836.

Configurez la liste de contrôle d'accès (ACL) et les captures de paquets :

```
ASAv(config)# access-list test_ipv6 extended permit ip any6 any6
ASAv(config)# cap capout interface outside access-list test_ipv6
```

Lancez une requête ping vers **fd02::1** à partir de l'ASA :

```
ASAv(config)# show cap capout
....
23: 10:55:10.275284 fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has
fd02::1 [class 0xe0]
24: 10:55:10.277588 fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1
[class 0xe0]
26: 10:55:11.287735 fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has
fd02::1 [class 0xe0]
27: 10:55:11.289642 fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1
[class 0xe0]
28: 10:55:12.293365 fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has
fd02::1 [class 0xe0]
29: 10:55:12.298538 fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1
[class 0xe0]
32: 10:55:14.283341 fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has
fd02::1 [class 0xe0]
33: 10:55:14.285690 fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1
[class 0xe0]
35: 10:55:15.287872 fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has
fd02::1 [class 0xe0]
36: 10:55:15.289825 fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1
[class 0xe0]
```

Comme indiqué dans les captures de paquets, les annonces de voisinage de **fd02::1** sont reçues.

Cependant, les annonces ne sont pas traitées pour une raison quelconque, comme indiqué dans les sorties de débogage. Pour plus d'informations, vous pouvez consulter les Syslogs.

Syslog ND

Voici quelques exemples de Syslogs ND :

```
May 13 2015 10:55:10: %ASA-7-609001: Built local-host identity:fd02::2
May 13 2015 10:55:10: %ASA-6-302020: Built outbound ICMP connection for faddr
ff02::1:ff00:1/0 gaddr fd02::2/0 laddr fd02::2/0(any)
May 13 2015 10:55:10: %ASA-3-325003: EUI-64 source address check failed.  Dropped
packet from outside:fd02::1/0 to fd02::2/0 with source MAC address c471.fe93.b516.
May 13 2015 10:55:10: %ASA-3-313008: Denied IPv6-ICMP type=136, code=0 from fd02::1
on interface outside
May 13 2015 10:55:11: %ASA-3-325003: EUI-64 source address check failed.  Dropped
packet from outside:fd02::1/0 to fd02::2/0 with source MAC address c471.fe93.b516.
May 13 2015 10:55:11: %ASA-3-313008: Denied IPv6-ICMP type=136, code=0 from fd02::1
on interface outside
May 13 2015 10:55:12: %ASA-3-325003: EUI-64 source address check failed.  Dropped
packet from outside:fd02::1/0 to fd02::2/0 with source MAC address c471.fe93.b516.
May 13 2015 10:55:12: %ASA-3-313008: Denied IPv6-ICMP type=136, code=0 from fd02::1
on interface outside
May 13 2015 10:55:14: %ASA-3-325003: EUI-64 source address check failed.  Dropped
packet from outside:fd02::1/0 to fd02::2/0 with source MAC address c471.fe93.b516.
May 13 2015 10:55:14: %ASA-3-313008: Denied IPv6-ICMP type=136, code=0 from fd02::1
on interface outside
May 13 2015 10:55:15: %ASA-3-325003: EUI-64 source address check failed.  Dropped
packet from outside:fd02::1/0 to fd02::2/0 with source MAC address c471.fe93.b516.
May 13 2015 10:55:15: %ASA-3-313008: Denied IPv6-ICMP type=136, code=0 from fd02::1
on interface outside
```

Dans ces syslogs, vous pouvez voir que les paquets d'annonce de voisin ND provenant de l'ISR à **fd02::1** sont abandonnés en raison de l'échec des vérifications de format EUI (Modified Extended Unique Identifier) 64 (Modified EUI-64).

> **Astuce** : Reportez-vous à la section *Modified EUI-64 Address Encoding* de ce document pour plus d'informations sur ce problème spécifique. Cette logique de dépannage peut également s'appliquer à tous les types de raisons de perte, par exemple lorsque les listes de contrôle d'accès n'autorisent pas ICMPv6 sur une interface spécifique ou lorsque des échecs de vérification de Unicast Reverse Path Forwarding (uRPF) se produisent, ce qui peut entraîner des problèmes de connectivité de couche 2 avec IPv6.

Dépannage du routage IPv6 de base

Les procédures de dépannage des protocoles de routage lorsque IPv6 est utilisé sont essentiellement les mêmes que lorsque IPv4 est utilisé. L'utilisation des commandes **debug** et **show**, ainsi que la capture de paquets, sont utiles pour tenter de déterminer la raison pour laquelle un protocole de routage ne se comporte pas comme prévu.

Débogues de protocole de routage pour IPv6

Cette section fournit les commandes de débogage utiles pour IPv6.

Débogues de routage IPv6 global

Vous pouvez utiliser le débogage **debug ipv6 routing** afin de dépanner toutes les modifications de la table de routage IPv6 :

```
ASAv# clear ipv6 ospf 1 proc

Reset OSPF process? [no]: yes
ASAv# IPv6RT0: ospfv3 1, Route update to STANDBY with epoch: 2 for
2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ospfv3 1, Delete 2001:aaaa:aaaa:aaaa::/64 from table
IPv6RT0: ospfv3 1, Delete backup for fd02::/64
IPv6RT0: ospfv3 1, Route update to STANDBY with epoch: 2 for ::/0
IPv6RT0: ospfv3 1, Delete ::/0 from table
IPv6RT0: ospfv3 1, ipv6_route_add_core for 2001:aaaa:aaaa:aaaa::/64 [110/10],
next-hop :: nh_source :: via interface outside route-type 2
IPv6RT0: ospfv3 1, Add 2001:aaaa:aaaa:aaaa::/64 to table
IPv6RT0: ospfv3 1, Added next-hop :: over outside for 2001:aaaa:aaaa:aaaa::/64,
[110/10]
IPv6RT0: ospfv3 1, ipv6_route_add_core Route update to STANDBY with epoch: 2 for
2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ipv6_route_add_core: input add 2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ipv6_route_add_core: output add 2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ospfv3 1, ipv6_route_add_core for fd02::/64 [110/10], next-hop ::
nh_source :: via interface outside route-type 2
IPv6RT0: ospfv3 1, ipv6_route_add_core for ::/0 [110/1], next-hop
fe80::c671:feff:fe93:b516
nh_source fe80::c671:feff:fe93:b516 via interface outside route-type 16
IPv6RT0: ospfv3 1, Add ::/0 to table
IPv6RT0: ospfv3 1, Added next-hop fe80::c671:feff:fe93:b516 over outside for ::/0,
[110/1]
IPv6RT0: ospfv3 1, ipv6_route_add_core Route update to STANDBY with epoch: 2 for ::/0
IPv6RT0: ipv6_route_add_core: input add ::/0
IPv6RT0: ipv6_route_add_core: output add ::/0
IPv6RT0: ospfv3 1, ipv6_route_add_core for 2001:aaaa:aaaa:aaaa::/64 [110/10],
next-hop :: nh_source :: via interface outside route-type 2
IPv6RT0: ospfv3 1, Route add 2001:aaaa:aaaa:aaaa::/64 [owner]
IPv6RT0: ospfv3 1, ipv6_route_add_core Route update to STANDBY with epoch: 2 for
2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ipv6_route_add_core: input add 2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ipv6_route_add_core: output add 2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ospfv3 1, ipv6_route_add_core for fd02::/64 [110/10], next-hop ::
nh_source :: via interface outside route-type 2
IPv6RT0: ospfv3 1, Reuse backup for fd02::/64, distance 110
IPv6RT0: ospfv3 1, ipv6_route_add_core for ::/0 [110/1], next-hop
fe80::c671:feff:fe93:b516 nh_source fe80::c671:feff:fe93:b516 via interface outside
route-type 16
IPv6RT0: ospfv3 1, Route add ::/0 [owner]
IPv6RT0: ospfv3 1, ipv6_route_add_core Route update to STANDBY with epoch: 2 for ::/0
IPv6RT0: ipv6_route_add_core: input add ::/0
IPv6RT0: ipv6_route_add_core: output add ::/0
```

Débogues OSPFv3

Vous pouvez utiliser la commande **debug ipv6 ospf** afin de résoudre les problèmes OSPFv3 :

```
ASAv# debug ipv6 ospf ?

adj OSPF adjacency events
database-timer OSPF database timer
```

```
events OSPF events
flood OSPF flooding
graceful-restart OSPF Graceful Restart processing
hello OSPF hello events
ipsec OSPF ipsec events
lsa-generation OSPF lsa generation
lsdb OSPF database modifications
packet OSPF packets
retransmission OSPF retransmission events
spf OSPF spf
```

Voici un exemple de sortie pour tous les débogages qui sont activés après le redémarrage du processus OSPFv3 :

```
ASAv# clear ipv6 ospf 1
OSPFv3: rcv. v:3 t:1 l:44 rid:192.168.128.115
aid:0.0.0.0 chk:a9ac inst:0 from outside
OSPFv3: Rcv hello from 192.168.128.115 area 0 from outside fe80::217:fff:fe17:af80
interface ID 142
OSPFv3: End of hello processingpr
OSPFv3: rcv. v:3 t:1 l:44 rid:14.38.104.1
aid:0.0.0.0 chk:bbf3 inst:0 from outside
OSPFv3: Rcv hello from 14.38.104.1 area 0 from outside fe80::c671:feff:fe93:b516
interface ID 14
OSPFv3: End of hello processingo
ASAv# clear ipv6 ospf 1 process

Reset OSPF process? [no]: yes
ASAv#
OSPFv3: Flushing External Links
Insert LSA 0 adv_rtr 172.16.118.1, type 0x4005 in maxage
OSPFv3: Add Type 0x4005 LSA ID 0.0.0.0 Adv rtr 172.16.118.1 Seq 80000029 to outside
14.38.104.1 retransmission list
....

!--- The neighbor goes down:

OSPFv3: Neighbor change Event on interface outside
OSPFv3: DR/BDR election on outside
OSPFv3: Elect BDR 14.38.104.1
OSPFv3: Elect DR 192.168.128.115
OSPFv3: Schedule Router LSA area: 0, flag: Change
OSPFv3: Schedule Router LSA area: 0, flag: Change
OSPFv3: Schedule Prefix DR LSA intf outside
OSPFv3: Schedule Prefix Stub LSA area 0
OSPFv3: 14.38.104.1 address fe80::c671:feff:fe93:b516 on outside is dead, state DOWN
....

!--- The neighbor resumes the exchange:

OSPFv3: Rcv DBD from 14.38.104.1 on outside seq 0xd09 opt 0x0013 flag 0x7 len 28
 mtu 1500 state EXSTART
OSPFv3: First DBD and we are not SLAVE
OSPFv3: rcv. v:3 t:2 l:168 rid:14.38.104.1
     aid:0.0.0.0 chk:5aa3 inst:0 from outside
OSPFv3: Rcv DBD from 14.38.104.1 on outside seq 0x914 opt 0x0013 flag 0x2 len 168
 mtu 1500 state EXSTART
OSPFv3: NBR Negotiation Done. We are the MASTER
OSPFv3: outside Nbr 14.38.104.1: Summary list built, size 0
OSPFv3: Send DBD to 14.38.104.1 on outside seq 0x915 opt 0x0013 flag 0x1 len 28
OSPFv3: rcv. v:3 t:2 l:28 rid:192.168.128.115
     aid:0.0.0.0 chk:295c inst:0 from outside
OSPFv3: Rcv DBD from 192.168.128.115 on outside seq 0xfeb opt 0x0013 flag 0x7 len 28
```

```
 mtu 1500 state EXSTART
OSPFv3: NBR Negotiation Done. We are the SLAVE
OSPFv3: outside Nbr 192.168.128.115: Summary list built, size 0
OSPFv3: Send DBD to 192.168.128.115 on outside seq 0xfeb opt 0x0013 flag 0x0 len 28
OSPFv3: rcv. v:3 t:2 l:28 rid:14.38.104.1
     aid:0.0.0.0 chk:8d74 inst:0 from outside
OSPFv3: Rcv DBD from 14.38.104.1 on outside seq 0x915 opt 0x0013 flag 0x0 len 28
 mtu 1500 state EXCHANGE
....

!--- The routing is re-added to the OSPFv3 neighbor list:

OSPFv3: Add Router 14.38.104.1 via fe80::c671:feff:fe93:b516, metric: 10
 Router LSA 14.38.104.1/0, 1 links
   Link 0, int 14, nbr 192.168.128.115, nbr int 142, type 2, cost 1
     Ignore newdist 11 olddist 10
```

Enhanced Interior Gateway Routing Protocol (EIGRP)

Le protocole EIGRP sur l'ASA ne prend pas en charge l'utilisation d'IPv6. Reportez-vous à la section Directives pour le protocole EIGRP du *livret 1 de l'interface de ligne de commande : Guide de configuration de l'interface de ligne de commande des opérations générales de la gamme Cisco ASA, 9.4* pour plus d'informations.

BGP (Border Gateway Protocol)

Cette commande **debug** peut être utilisée afin de dépanner BGP quand IPv6 est utilisé :

```
ASAv# debug ip bgp ipv6 unicast  ?

X:X:X:X::X IPv6 BGP neighbor address
keepalives BGP keepalives
updates BGP updates
<cr>
```

Commandes show utiles pour IPv6

Vous pouvez utiliser ces commandes **show** afin de résoudre les problèmes IPv6 :

- **show ipv6 route**
- **show ipv6 interface brief**
- **show ipv6 ospf <ID de processus>**
- **show ipv6 traffic**
- **show ipv6 neighbor**
- **show ipv6 icmp**

Packet Tracers avec IPv6

Vous pouvez utiliser la fonctionnalité Packet Tracer intégrée avec IPv6 sur l'ASA de la même

manière qu'avec IPv4. Voici un exemple où la fonctionnalité packet-tracer est utilisée afin de simuler l'hôte interne à **fd03::2**, qui tente de se connecter à un serveur Web **555::1** situé sur Internet avec la route par défaut apprise de l'interface **881** via OSPF :

```
ASAv# packet-tracer input inside tcp fd03::2 10000 5555::1 80 detailed

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7fffd59ca0f0, priority=1, domain=permit, deny=false
       hits=2734, user_data=0x0, cs_id=0x0, l3_type=0xdd86
       src mac=0000.0000.0000, mask=0000.0000.0000
       dst mac=0000.0000.0000, mask=0100.0000.0000
       input_ifc=inside, output_ifc=any

Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop fe80::c671:feff:fe93:b516 using egress ifc  outside

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7fffd589cc30, priority=1, domain=nat-per-session, deny=true
       hits=1166, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0,
protocol=6
       src ip/id=::/0, port=0, tag=any
       dst ip/id=::/0, port=0, tag=any
       input_ifc=any, output_ifc=any

<<truncated output>>

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow

ASAv#
```

Notez que l'adresse MAC de sortie est l'adresse link-local de l'interface 881. Comme mentionné précédemment, pour de nombreux protocoles de routage dynamique, les routeurs utilisent des adresses IPv6 link-local afin d'établir des contiguïtés.

Liste complète des débogages ASA liés à IPv6

Voici les débogages qui peuvent être utilisés pour résoudre les problèmes IPv6 :

```
ASAv# debug ipv6 ?

dhcp IPv6 generic dhcp protocol debugging
dhcprelay IPv6 dhcp relay debugging
icmp ICMPv6 debugging
interface IPv6 interface debugging
mld IPv6 Multicast Listener Discovery debugging
nd IPv6 Neighbor Discovery debugging
ospf OSPF information
packet IPv6 packet debugging
routing IPv6 routing table debugging
```

Problèmes courants liés à IPv6

Cette section décrit comment résoudre les problèmes les plus courants liés à l'IPv6.

Sous-réseaux mal configurés

De nombreux cas de TAC IPv6 sont générés en raison d'un manque général de connaissances sur le fonctionnement d'IPv6 ou de tentatives d'implémentation d'IPv6 par l'administrateur à l'aide de processus spécifiques à IPv4.

Par exemple, le centre d'assistance technique a constaté des cas où un bloc \56 d'adresses IPv6 a été attribué à un administrateur par un fournisseur d'accès Internet (FAI). L'administrateur attribue ensuite une adresse et le sous-réseau \56 complet à l'interface externe ASA et choisit une plage interne à utiliser pour les serveurs internes. Cependant, avec IPv6, tous les hôtes internes doivent également utiliser des adresses IPv6 routables et le bloc d'adresses IPv6 doit être divisé en sous-réseaux plus petits selon les besoins. Dans ce scénario, vous pouvez créer de nombreux \64 sous-réseaux dans le bloc \56 qui a été alloué.

> **Astuce** : Référez-vous à RFC 4291 pour plus d'informations.

Codage EUI 64 modifié

L'ASA peut être configuré afin de nécessiter des adresses IPv6 codées EUI-64 modifiées. L'interface EUI, conformément à la RFC 4291, permet à un hôte de s'attribuer un identificateur d'interface IPv6 unique de 64 bits (EUI-64). Cette fonctionnalité est un avantage par rapport à IPv4, car elle supprime l'obligation d'utiliser DHCP pour l'attribution d'adresse IPv6.

Si l'ASA est configuré afin d'exiger cette amélioration via la commande **ipv6 Enforcement-eui64 nameif**, alors il abandonnera probablement de nombreuses sollicitations et annonces de découverte de voisin d'autres hôtes sur le sous-réseau local.

> **Astuce** : Pour plus d'informations, reportez-vous au document Présentation de l'adresse IPv6 EUI-64 bits de la communauté d'assistance Cisco.

Les clients utilisent des adresses IPv6 temporaires par défaut

Par défaut, de nombreux systèmes d'exploitation (OS) clients, tels que Microsoft Windows versions 7 et 8, Macintosh OS-X et systèmes basés sur Linux, utilisent des adresses *temporaires* IPv6 auto-attribuées pour une confidentialité étendue via la configuration automatique des adresses sans état IPv6 (SLAAC).

Le centre d'assistance technique de Cisco a constaté des cas où cela a causé des problèmes inattendus dans les environnements, car les hôtes génèrent du trafic à partir de l'adresse temporaire et non de l'adresse attribuée de manière statique. Par conséquent, les listes de contrôle d'accès et les routes basées sur l'hôte peuvent entraîner l'abandon ou le routage incorrect du trafic, ce qui entraîne l'échec de la communication de l'hôte.

Deux méthodes sont utilisées pour remédier à cette situation. Le comportement peut être désactivé individuellement sur les systèmes clients, ou vous pouvez désactiver ce comportement sur les routeurs ASA et Cisco IOS®. Du côté de l'ASA ou du routeur, vous devez modifier l'indicateur de message d'annonce de routeur (RA) qui déclenche ce comportement.

Reportez-vous aux sections suivantes afin de désactiver ce comportement sur les systèmes de clients individuels.

Microsoft Windows

Complétez ces étapes afin de désactiver ce comportement sur les systèmes Microsoft Windows :

1. Dans Microsoft Windows, ouvrez une invite de commandes élevée (exécutez en tant qu'administrateur).

2. Entrez cette commande afin de désactiver la fonction de génération aléatoire d'adresses IP, puis appuyez sur **Entrée** :

   ```
   netsh interface ipv6 set global randomizeidentifiers=disabled
   ```

3. Entrez cette commande afin de forcer Microsoft Windows à utiliser la norme EUI-64 :

   ```
   netsh interface ipv6 set privacy state=disabled
   ```

4. Redémarrez la machine afin d'appliquer les modifications.

Macintosh OS-X

Dans un terminal, entrez cette commande afin de désactiver IPv6 SLAAC sur l'hôte jusqu'au prochain redémarrage :

```
sudo sysctl -w net.inet6.ip6.use_tempaddr=0
```

Afin de rendre la configuration permanente, entrez cette commande :

```
sudo sh -c 'echo net.inet6.ip6.use_tempaddr=0 >> /etc/sysctl.conf'
```

Linux

Dans un interpréteur de commandes terminal, entrez cette commande :

```
sysctl -w net.ipv6.conf.all.use_tempaddr=0
```

Désactiver SLAAC globalement à partir de l'ASA

La deuxième méthode utilisée pour traiter ce comportement est de modifier le message RA envoyé par l'ASA aux clients, ce qui déclenche l'utilisation de SLAAC. Afin de modifier le message RA, entrez cette commande à partir du mode *Configuration de l'interface* :

```
ASAv(config)# interface gigabitEthernet 1/1
ASAv(config-if)# ipv6 nd prefix 2001::db8/32 300 300 no-autoconfig
```

Cette commande modifie le message RA envoyé par l'ASA de sorte que l'indicateur de bit A ne soit pas défini et que les clients ne génèrent pas d'adresse IPv6 temporaire.

> **Astuce** : Référez-vous à RFC 4941 pour plus d'informations.

FAQ sur IPv6

Cette section décrit quelques questions fréquemment posées concernant l'utilisation d'IPv6.

Puis-je transmettre simultanément le trafic IPv4 et IPv6 sur la même interface ?

Oui. Vous devez simplement activer IPv6 sur l'interface et attribuer une adresse IPv4 et une adresse IPv6 à l'interface, et il gère les deux types de trafic simultanément.

Puis-je appliquer les listes de contrôle d'accès IPv6 et IPv4 à la même interface ?

Vous pouvez effectuer cette opération dans les versions ASA antérieures à la version 9.0(1). Depuis la version 9.0(1) d'ASA, toutes les listes de contrôle d'accès sur l'ASA sont *unifiées*, ce qui signifie qu'une liste de contrôle d'accès prend en charge un mélange d'entrées IPv4 et IPv6 dans la même liste de contrôle d'accès.

Dans les versions 9.0(1) et ultérieures d'ASA, les listes de contrôle d'accès sont simplement fusionnées et la liste de contrôle d'accès unique et unifiée est appliquée à l'interface via la commande **access-group**.

L'ASA prend-il en charge la QoS pour IPv6 ?

Oui. L'ASA prend en charge la réglementation et la mise en file d'attente par priorité pour IPv6 de la même manière qu'avec IPv4.

Depuis la version 9.0(1) d'ASA, toutes les listes de contrôle d'accès sur l'ASA sont *unifiées*, ce qui signifie qu'une liste de contrôle d'accès prend en charge un mélange d'entrées IPv4 et IPv6 dans la même liste de contrôle d'accès. Par conséquent, toute commande QoS appliquée sur une carte de classe qui correspond à une liste de contrôle d'accès prend des mesures sur le trafic IPv4 et IPv6.

Dois-je utiliser NAT avec IPv6 ?

Bien que la NAT puisse être configurée pour IPv6 sur l'ASA, l'utilisation de la NAT dans IPv6 est fortement découragée et inutile, étant donné la quantité quasi infinie d'adresses IPv6 disponibles et routables globalement.

Si la NAT est requise dans un scénario IPv6, vous trouverez plus d'informations sur la façon de la configurer dans la section Instructions NAT IPv6 du *manuel CLI Book 2 : Guide de configuration CLI du pare-feu de la gamme Cisco ASA, 9.4*.

> **Note**: Il y a des directives et des limitations qui doivent être prises en compte lors de l'implémentation de NAT avec IPv6.

Pourquoi les adresses IPv6 link-local apparaissent-elles dans la sortie de la commande *show failover* ?

Dans IPv6, ND utilise des adresses link-local afin d'exécuter la résolution d'adresse de couche 2. Pour cette raison, les adresses IPv6 des interfaces surveillées dans le résultat de la commande **show failover** affichent l'adresse link-local et non l'adresse IPv6 globale configurée sur l'interface. C'est un comportement attendu.

Demandes d'amélioration/de cavernes connues

Voici quelques mises en garde connues concernant l'utilisation d'IPv6 :

- ID de bogue Cisco CSCtn09836 â â' suffi *clause de correspondance de capture ASA 8.x n'intercepte pas le trafic IPv6*
- Identifiant de bogue Cisco CSCuq85949 â âsuffi *ENH : Prise en charge ASA IPv6 pour WCCP*
- ID de bogue Cisco CSCut78380 â â suffixe *le routage ECMP IPv6 ASA n'équilibre pas la charge du trafic*

Informations connexes

- RFC 2460 - - Spécification Protocole Internet, Version 6 (IPv6)
- RFC 4291 - - Architecture d'adressage IP version 6
- RFC 4861 - - Découverte voisin pour IP version 6 (IPv6)
- CII Book 1 : Guide de configuration de l'interface de ligne de commande des opérations générales de la gamme Cisco ASA, 9.4 - - IPv6

- Configuration d'AnyConnect SSL sur IPv4+IPv6 vers ASA
- Support technique et documentation - - Cisco Systems